**.**

**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

Data integrity is the assurance that data is accurate and reliable.

Biometrics

* 1. Describe biometric security.

Biometric security is the use of physical human characteristics.

* 1. Why does it appeal to security managers?

It appeals to security managers because it is nearly impossible to copy or steal a persons biometric characteristics.

* 1. List the common biometric devices.
     + Voice recognition
     + Fingerprint recognition
     + Hand geometry
     + Signature verification
     + Facial recognition
     + Iris recognition
  2. What are the concerns of biometric technology?

The main concern would be the perceived intrusiveness of the technology.

1. Swipe cards
   1. Describe the nature of a swipe card.

The nature of a swipe card is a business card sized plastic card with a magnetic strip on one side and user details stamped or printed on the other.

* 1. What is a limitation of the swipe card?

One limitation is that it can be easily damaged by magnetic fields.

1. Smart cards
2. Security tokens
3. Mobile phone secure code
   1. How does this level of authentication work?

It works by sending a security code to the account holders mobile phone to authenticate a transaction before it happens.

**Power protection**

Outline the characteristics of the following:

1. Surge protector
2. Uninterruptible power supply, (UPS)

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?
2. What is meant be a fault-tolerant server?
3. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.
   2. What is meant by RAID technology
4. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

Three categories of backup media:

* Magnetic media
* Optical drives
* Solid-state drives

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

* Affordable
* Useful if you have many files
* Destroyed easily by things such as a fire or flood

1. Magnetic tapes

* Cheap
* Very slow
* Where time is not an issue it provides a cheaper and larger capacity then a CD or DVD

**Optical media**

1. Compact disc

* Removable
* Can hold up to 700 mb of data

1. DVD

* Can store up 17GB(double sided) of data
* DVD-R can only be used once
* DVD-RW can be used many times

1. Blu-ray

* Capacity of 50GB (dual layer)
* Disc is read by blue laser
* Allows storage of high definition films

**Solid-state drives**

1. USB storage devices

* Small
* No moving parts
* Can hold up to 256GB

**Online backups**

1. Why do organisations use this form of backup?

They use this form of backup because they have fault tolerant servers, redundant power supplies, multiple internet connections and uninterruptible power supplies.

1. Describe an enterprise storage system.

An enterprise storage system is a storage system that uses a variety of storage techniques to ensure its data is secure.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

Packet sniffers are diagnostic tools that monitor the contents of packets of data being sent across networks.

1. Desktop monitoring programs

Desktop monitoring programs work by intercepting every single action performed on a computer.

1. Log files

Log files record what we do. Like our own web browsers store web sites that have been accessed.

1. Closed-circuit television, (CCTV)

Closed-circuit television consists of a series of video cameras linked to an internal TV system.

1. Telephones

Just like in the spy films where the police listen in or ‘tap’ into a phone conversation.

1. Audit trails

Audit trails are the combination of surveillance systems described above enable managers to trace transactions or any other form of activity in the system.

**Physical security devices:** List the options for physically securing your data

* Lockable disc box
* Store removable hard drives in a safe
* Cable lock laptops